APPARATUS AND METHODS FOR UNLOCKING PASSWORD PROTECTED SOFTWARE SYSTEMS TO RECOVER MASTER PASSWORD

RELATED APPLICATION

This application claims the benefit of provisional Application No. 60/100,753 filed September 17, 1998, the disclosure of which is incorporated fully herein.

FIELD OF THE INVENTION

The present invention relates generally to password protected software systems, and more particularly, to password protected software systems with on screen display, such as parental control-equipped electronic programming guide systems for television viewing.

BACKGROUND OF THE INVENTION

Many software systems require the user to enter a password before the system will allow the user to access the system. Passwords must be recognized by the software system as giving the user authority to access the system. An example of a password protected software system is a parental control-equipped electronic programming guide system such as Gemstar's Guide Plus+ 99 equipped with V-Chip Plus+ In-Guide User Interface.

It is typically the responsibility of the user to remember the user's own password. If a user forgets the password, the user cannot access the system until the user again learns the password.

Some password protected software systems are available on a network. In a networked system, there is typically a network administrator, online service provider, or the like, that establishes initial passwords, and assists the user in identifying a forgotten password.

In many password protected software systems, the user is provided a first-time password by the network administrator, online service provider, or manufacturer. When the user tries to access the system, the system prompts the user for the user's password. Some systems are programmed to recognize if the password is a "first-time" password. When the system detects a first-time password, the system prompts the user to choose a personal password. Alternatively, the "first-time" password is set to expire within a relatively short period of time or after a relatively short number of accesses. Systems are typically programmed to recognize the expiration date of a password and notify the user that the user must select a new password before the old password expires.

If the user forgets the chosen password, in the case of many online network systems, a systems or network administrator can typically recover the identification of the forgotten

password for the user. The systems or network administrator, who is typically at a location remote from the user, can check security files internal to the system. By reading the internal security files, the systems or network administrator can provide the user with the user's password. Before disclosing the password, the systems administrator typically requires that the user provide the systems administrator with the proper identification.

On the other hand, in the case of a system that is not networked, or in the case where the systems software is not accessible by the user or by a systems or network administrator, the password, once set, is known only to the system. In the present application, such systems will hereinafter be referred to as "local systems." An example of a local system is an on screen system for parental control of television viewing such as Gemstar's Guide Plus+ 99 equipped with V-Chip Plus+ In-Guide User Interface.

With a local system, there is no network administrator that can read the files from a location remote from the user and provide the user with the chosen password. With such a local system, a user could uncover the forgotten password by dismantling the device; detaching the system hardware component that contains the password (e.g., RAM storage); and sending the component to the manufacturer for analysis. This is a cumbersome and impractical solution.

Another way to provide the user with the ability to recover the identity of a forgotten password would be to allow the user to access the password. That is, the user could select an option in the system that would display the password. However, such a method would be self-defeating, in that others could equally access the password.

Still another way to provide the user with the ability to recover the identity of a forgotten password would be to provide a "back door" method, such as: unplugging and replugging the television; or pressing a combination of input keys, such as the keys on a television remote control device. However, such "back door" methods could quickly become discovered; as more and more households adapt the password protected system, such back door methods would become widely known.

Because it is inevitable that some users will, from time to time, forget their passwords, some method and apparatus for a user to recover a forgotten password is needed while maintaining the security and integrity of the protected software system.

SUMMARY OF THE INVENTION

The present invention provides apparatus and methods that satisfy these needs. Specifically, the present invention provides apparatus and methods for recovering a forgotten password while maintaining the security and integrity of the protected software system. In particular, the present invention provides for a centralized contact, hereinafter referred to as

the "central administrator" or "central administration." The present invention further provides for the identification of the particular user to the particular local system, the identification of the particular local system to the central administrator, and the identification of the particular user to the central administrator. After providing all of the above-described proper identifications, the present invention provides for the identification of the forgotten password to the central administrator who then provides the forgotten password to the user.

Alternatively, the invention provides for the identification by the central administrator of a key that will unlock the software system for the user so that the user can access the identification of the user's password.

The procedure of identifying a forgotten password is generally referred to hereinafter in this application as the master password recovery procedure.

DESCRIPTION OF THE DRAWINGS

These and other features, aspects, and advantages of the present invention will become better understood with regard to the following description, appended claims, and accompanying drawings where:

FIG. 1 is a graphical representation of one embodiment of a local system implementation of an on screen setup procedure display requesting input of the personal identification information for a user and the user's selection of a master password;

FIG. 2 is a flow diagram of one embodiment of a local system implementation of the master password setup procedure;

FIG. 3 is a graphical representation of one embodiment of a local system implementation of an on screen display of a master password recovery instruction screen.

FIG. 4 is a flow diagram of one embodiment of a local system implementation of the master password recovery procedure.

DETAILED DESCRIPTION OF THE INVENTION

A central administration contact, hereinafter referred to in this application as the central administrator, is established. The central administrator would be accessible by the user, through, *e.g.*, a 1-800, or 1-900 telephone number, a website, etc. In the preferred embodiment, the central administration contact is a completely automated Computer Telephone Interface system. In the preferred embodiment, the automated central administration system provides vocal communications to the user and requests that the user provide input to the central administrator by pressing buttons on the user's telephone keypad. Alternatively, the automated central administration system is programmed to recognize speech so that the user can speak to the central administration system to provide requested

information.

A. MASTER PASSWORD SETUP PROCEDURE

When the user attempts to access the local system, the local system will prompt the user for the password. Typically, the first time that a password protected system is accessed, the system will allow the user to identify a password. This password is hereinafter referred to in this application as a "master password."

Alternatively, the manufacturer may provide the buyer of the system with a first-time password. FIG. 2 is a flow diagram of one embodiment of a local system implementation of the master password setup procedure where the user has been supplied a first-time password.

When the local system is first accessed, the user/buyer is prompted to supply the first-time password 210. Input of the password and other user input referred to herein may be accomplished using a variety of devices 230 and 450, including but not limited to an infra-red remote control device, such as a television remote control 232a, 233a, 235a and 452a, or a keyboard 232b, 233b, 235b and 452b. The input device used is not a limitation of the present invention.

Once the user/buyer supplies the first-time password 220 and 232a and 232b, the system will typically invite the user to choose a personal master password 250. Once the user chooses and inputs the master password 270 and FIG. 1, 80, the local system typically asks the user to confirm the master password by entering it a second time (not shown). If the user is unable to confirm the password, the local system typically reverts to the first-time password and the procedure starts all over again. The above-described procedure will be referred to hereinafter in this application as the "master password setup procedure."

During the master password setup procedure, one embodiment of the present invention requires that the user provide some additional identification information. This information would be information that would be known to the user but not typically known to others, such as, *e.g.*, the user's mother's maiden name, the user's mother's birth date, or other such personal information.

FIG. 1 is a graphical representation of one embodiment of a local system implementation of an on screen setup procedure display requesting input of the personal identification information for a user and the user's selection of a master password. In this embodiment, the user is invited to use a pull down menu (not shown) of the alphabet, special characters, and the numbers 0-9, or some other comparable method, to compose the user's input to the personal identification information screen. The personal identification information, to the extent that a particular embodiment of the present invention requires this information, will be referred to hereinafter in this application as "master password

identification information." In FIG. 1, the embodiment of the setup procedure display screen depicted requests the user to input the user's first name (10), the user's middle initial (20), the user's last name (30), the user's birth date in MM/DD/YYYY format (40), the user's mother's maiden name (50), and the user's mother's birth date in MM/DD/YYYY format (60). The setup procedure display screen depicted provides for the user the serial number of the unit (70). In one embodiment, the serial number is encrypted through a hashing function. The user is also requested to input a selected Master Password (80).

In one embodiment of the invention, the master password setup procedure instructs the user to contact the central administrator to provide certain user identification information 280. This further personal identification information may be in the way of a credit card number, or may be the same as the master password identification information or may include some personal identification information in addition to the master password identification information. This further personal identification information is referred to hereinafter in this application as "counter-identification information."

In one embodiment of the invention, the master password setup procedure requires confirmation from the central administrator that the counter-identification information has been provided. In this embodiment, the local system and the central administration system each use the same hashing function to each calculate a confirmation key. The central administration computer system (or alternatively, the manual procedure to be performed by the central administrator) and the local system are both programmed to perform a hashing function on information already "known" to the television, for instance, the date, day of the week, zip code of the location of the television, the cable or other programming service to which the television is connected, the serial number of the television, etc. In an alternative embodiment, the hashing function could be programmed to incorporate as part of the calculation of the hashing key, information that was provided to both the local system and to the central administrator by the user as part of the identification information.

The central administrator uses the central administration system to calculate the appropriate confirmation key. The local system calculates the corresponding confirmation key 290. The user would then be instructed to enter the confirmation key provided by the central administrator into the local system 235a and 235b. The local system would read the confirmation key input by the user 305. The local system would compare the input confirmation key with the key that had been calculated by the local system 310. If the two keys match, then the local system allows the user to proceed with the master password setup procedure 320.

B. MASTER PASSWORD CHANGE PROCEDURE

Most password protected systems allow the user to change the password after it has been established. Password change procedures typically require that the user identify the current password before entering the new password; once the new password has been entered, password change procedures typically require the user to confirm the new password by entering the new password a second time. Such a password change procedure is also included in references herein to the "master password setup procedure."

C. PASSWORD PROTECTION AND MASTER PASSWORD RECOVERY

Every time after completing the master password setup procedure, whenever the user tries to access the local system, or in some embodiments, whenever the user tries to access protected blocked areas of the system, the local system prompts the user to supply the master password. If the user is unable to provide the master password, the system will not allow the user to pass the security screen of the system.

At this point, the invention provides that the user can access security processing for the local system. Specifically, the invention provides for a master password recovery process. FIG. 3 is a graphical representation of one embodiment of a local system implementation of an on screen display of a master password recovery instruction screen. FIG. 4 is a flow diagram of one embodiment of a local system implementation of the master password recovery procedure. In an alternative embodiment, the user will refer to a user manual or contact the manufacturer or retailer to identify contact information for the central administration system.

The local system security processor will ask the user to supply the master password identification information, to the extent that this information was requested during the master password setup procedure. The screen that requests the identification information will look like the setup screen, one embodiment of which is depicted in FIG. 1.

Once the requested information has been input, the security system will display a screen that will instruct the user to access the central administrator. This screen is hereinafter referred to as the "instruction screen." As seen in FIG. 3, the instruction screen will tell the user how to contact the central administrator (100), *e.g.*, to dial a particular telephone number, such as a 1-900 number, 1-800 number, or to access a particular website. The instruction screen will display information identifying the particular local system unit, such as the serial number of the particular local system unit (110, 405-410). In one embodiment, the instruction screen will also display a character string (120, 420-430). In one embodiment, the character string displayed will be encrypted and will contain, among other things, the forgotten master password, and to the extent that any was been requested by the local system,

the master password identification information.

Once the user contacts the central administrator, the central administrator will request that the user read from the instruction screen certain information, such as: device unit identification information (110), for example, the serial number of the particular local system unit; and/or other information displayed on the user's local system screen, such as an encrypted character string (120). In one embodiment, the central administrator will further request that the user provide the counter-identification information previously provided to the central administrator during the master password setup procedure.

The central administrator will then use the information provided by the user to either provide the user with the user's master password, or with a key to unlock the user's system to, depending upon the embodiment, discover the forgotten master password, or to choose a new master password. The central administrator's function may be manually performed, or alternatively, may be programmed in the central administration computer system.

Depending on the embodiment, the central administrator may need to de-encrypt the information provided by the user. To de-encrypt the user-provided information, the central administrator may use a manual procedure or may enter the information into the central administration computer system which is programmed to de-encrypt the user-provided information. Depending on the embodiment, the central administrator will then test the de-encrypted master password identification information against the counter-identification information. This comparison procedure may be either a manual procedure performed by the central administrator or may be performed by the central administration computer system.

In an embodiment in which the user reads to the central administrator an encrypted character string containing an encrypted master password, once the central administrator has determined that the identification information is in order, the central administrator will de-encrypt the character string to identify the forgotten password. In one embodiment of the invention, the central administrator will then instruct the user to request the system to calculate a confirmation key. To do that, the user will choose an on screen option to calculate a confirmation key. In one embodiment, the local system will automatically calculate 440 and 490 a confirmation key (130) and/or a counter-confirmation key (140). The security information system will display a screen that says that a confirmation key has been calculated (see FIG. 3, 130). The central administrator will then calculate a confirmation key and instruct the user to input the confirmation key. The user will then use a pull down menu (not shown), or some other comparable method, to input the confirmation key. Once the user has input the confirmation key, the local system will test the two keys. If the key matches the local system confirmation key, the system will then display on screen a counter-confirmation key (140 and 500) and instruct the user to read the counter-

confirmation key to the central administrator. In one embodiment, the local system will then set the master password to expire after a set period of time, *e.g.*, a day, 48 hours, a week, a month, or after a set number of accesses, e.g., after 1, 2 or 3 further accesses by the user of the local system.

The central administrator will then tell the user the forgotten password.

In an alternative embodiment of the present invention, the central administrator, as described above, will calculate a confirmation key and instruct the user to input the confirmation key into the local system. The user will then use a pull down menu (not shown) or some other comparable method to input the confirmation key. Once the user has input the confirmation key, the local system will calculate, using the same hashing function used by the central administrator, a local system confirmation key. The local system will then test the two keys. If the key matches the local system confirmation key, the system will then display on screen the user's master password (similar to 140 and 500).

In another alternative embodiment of the present invention, the central administrator, as described above, will calculate a key, using, e.g., a hashing formula, that will unlock the user's system. The central administrator will then instruct the user to input the unlocking key. The user will then use a pull down menu (not shown) or some other comparable method to input the unlocking key. Once the user has input the unlocking key, the local system will calculate, as described above, a key, using, e.g., a hashing formula. The local system uses the same hashing formula as is used by the central administrator and/or the central administration computer system. In order for the two keys to match, the hashing formula must be applied by the local system to the same information to which the central administrator's hashing formula was applied. If the unlocking key matches the local system key, the local system will then display on screen the user's master password (similar to 140 and 500). In an alternative embodiment, in the case where the keys match, the local system will require that the user immediately identify a new master password.

D. AN ILLUSTRATIVE EMBODIMENT OF MASTER PASSWORD RECOVERY IN A V-CHIP PLUS+ IN-GUIDE USER INTERFACE.

As an illustrative embodiment of the present invention, the master password setup procedure and the master password recovery procedure described above are implemented in the following manner to allow a parent to unlock and recover the parent's master password that governs a parental control-equipped electronic programming guide system such as Gemstar's Guide Plus+ 99 equipped with V-Chip Plus+ In-Guide User Interface.

The parent/user purchases a television equipped with a parental control-equipped electronic programming guide system such as Gemstar's Guide Plus+ 99 equipped with V-

Chip Plus+ In-Guide User Interface. The first time that the parent connects the television to a power supply and turns the system on, the parent is prompted through an initial setup procedure that includes a master password setup procedure. As part of the master password setup procedure, the user/parent identifies a master password.

Later, in the event that the user/parent forgets the master password, the user/parent selects a security system option that displays a screen (the "instruction screen") on the television display monitor that instructs the user/parent to contact a central administrator through a 1-900 telephone number. The central administrator in this embodiment is a completely automated Computer Telephone Interface system.

In an alternative embodiment, the user/parent refers to a user manual or contacts the manufacturer or retailer to identify contact information for the central administration system.

The central administration one-way hashing function will be performed on the current date to calculate an unlocking key. Alternatively, the central administrator, once contacted, may ask the user to supply the television's serial number, and possibly, some other types of information as was described previously in this application. The user/parent will be instructed to enter the requested information using the user/parent's telephone key pad. Other types of information requested would be information that would be "known" to the television set, such as, e.g., the zip code of the location of the television set, the cable service or other programming service to which the television is connected, etc.

The central administration computer system will then use a one-way hashing function to calculate an unlocking key. The central administration computer system will read the unlocking key to the user/parent and instruct the user/parent to enter the unlocking key into the user/parent's local television V-Chip Plus+ In-Guide User Interface system.

After the user/parent has entered the unlocking key into the local system, the local system will calculate an unlocking key using the same one-way hashing function as was used by the central administration computer system. The local system will then compare the two keys.

If the two keys match, the local television V-Chip Plus+ In-Guide User Interface system will then display on the television display monitor instructions to the user/parent to immediately choose a new master password. The user/parent must then use the appropriate keys on the viewer's remote control device to identify a new master password. Once the user/parent has identified a new master password, the local system replaces the old master password in the system security files with the new master password and allows the user/parent to proceed with accessing local system functions.

As an optional feature, the user's system displays notification on the television display monitor notifying the user that the master password has been changed. The notification may

be displayed in the form of an information screen, insert, overlay, scrolling message, or other such notification. The notification would be displayed every time the user turns the television on for a certain number of times, or alternatively, for a certain number of days.

Illustrative Embodiments.

The embodiments of the invention described herein are only considered to be preferred and/or illustrative of the inventive concept; the scope of the invention is not to be restricted to such embodiments. Various and numerous other arrangements may be devised by one skilled in the art without departing from the spirit and scope of this invention. For example, the present invention can be implemented using a completely automated central administration system capable of recognizing user information input with the user's telephone keypad or capable of recognizing user speech. Alternatively, the present invention can be implemented using a partially or completely manual central administration contact.